PCT/EP200 4 / 0 5 0 8 8 9

The Patent Office

INVESTOR IN PEOPLE

0 2 JUL 2004

The Patent Office
Concept House
Cardiff Road
Newport
South Wales
NP10 8QQ

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

REC'D 13 AUG 2004
WIPO PCT

I, the undersigned, being an officer duly authorised in accordance with Section 74(1) and (4) of the Deregulation & Contracting Out Act 1994, to sign and issue certificates on behalf of the Comptroller-General, hereby certify that annexed hereto is a true copy of the documents as originally filed in connection with the patent application identified therein.

In accordance with the Patents (Companies Re-registration) Rules 1982, if a company named in this certificate and any accompanying documents has re-registered under the Companies Act 1980 with the same name as that with which it was registered immediately before re-registration save for the substitution as, or inclusion as, the last part of the name of the words "public limited company" or their equivalents in Welsh, references to the name of the company in this certificate and any accompanying documents shall be treated as references to the name with which it is so re-registered.

In accordance with the rules, the words "public limited company" may be replaced by p.l.c., plc, P.L.C. or PLC.

Re-registration under the Companies Act does not constitute a new legal entity but merely subjects the company to certain additional company law rules.

Signed P. Mahoney

Dated 14 June 2004

Patents Form 1/77

Patents Act 1977
(Rule 16)

The Patent Office

Request for grant of a patent

(See the notes on the back of this form. You can also get an explanatory leaflet from the Patent Office to help you fill in this form)

The Patent Office

Cardiff Road
Newport
South Wales
NP9 1RH

1. Your reference — RL.P52728GB

2. Patent application number *(The Patent Office will fill in this part)* — 0311921.1 — 23 MAY 2003

3. Full name, address and postcode of the or of each applicant *(underline all surnames)*

Telefonaktiebolaget LM Ericsson (Publ)
SE-12625
Stockholm
Sweden

Patents ADP number *(if you know it)* 78503990 01

If the applicant is a corporate body, give the country/state of its incorporation — Sweden

4. Title of the invention — Mobile Security

5. Name of your agent *(if you have one)* — Marks & Clerk

"Address for service" in the United Kingdom to which all correspondence should be sent *(including the postcode)*

4220 Nash Court
Oxford Business Park South
Oxford OX4 2RU
United Kingdom

Patents ADP number *(if you know it)* — 7271125001

6. If you are declaring priority from one or more earlier patent applications, give the country and the date of filing of the or of each of these earlier applications and *(if you know it)* the or each application number

Country	Priority application number *(if you know it)*	Date of filing *(day / month / year)*

7. If this application is divided or otherwise derived from an earlier UK application, give the number and the filing date of the earlier application

Number of earlier application	Date of filing *(day / month / year)*

8. Is a statement of inventorship and of right to grant of a patent required in support of this request? *(Answer 'Yes' if:*
a) any applicant named in part 3 is not an inventor, or
b) there is an inventor who is not named as an applicant, or
c) any named applicant is a corporate body.
See note (d)) — Yes

Patents Form 1/77

9. Enter the number of sheets for any of the following items you are filing with this form. Do not count copies of the same document

Continuation sheets of this form	
Description	7
Claim(s)	0
Abstract	0
Drawing(s)	0

10. If you are also filing any of the following, state how many against each item.

Priority documents	
Translations of priority documents	
Statement of inventorship and right to grant of a patent *(Patents Form 7/77)*	
Request for preliminary examination and search *(Patents Form 9/77)*	
Request for substantive examination *(Patents Form 10/77)*	
Any other documents *(please specify)*	

11. I/We request the grant of a patent on the basis of this application.

Signature Marks & Clerk Date 22 May 2003

12. Name and daytime telephone number of person to contact in the United Kingdom

Dr. Robert Lind
01865-397900

Warning

After an application for a patent has been filed, the Comptroller of the Patent Office will consider whether publication or communication of the invention should be prohibited or restricted under Section 22 of the Patents Act 1977. You will be informed if it is necessary to prohibit or restrict your invention in this way. Furthermore, if you live in the United Kingdom, Section 23 of the Patents Act 1977 stops you from applying for a patent abroad without first getting written permission from the Patent Office unless an application has been filed at least 6 weeks beforehand in the United Kingdom for a patent for the same invention and either no direction prohibiting publication or communication has been given, or any such direction has been revoked.

Notes

a) *If you need help to fill in this form or you have any questions, please contact the Patent Office on 0645 500505.*

b) *Write your answers in capital letters using black ink or you may type them.*

c) *If there is not enough space for all the relevant details on any part of this form, please continue on a separate sheet of paper and write "see continuation sheet" in the relevant part(s). Any continuation sheet should be attached to this form.*

d) *If you have answered 'Yes' Patents Form 7/77 will need to be filed.*

e) *Once you have filled in the form you must remember to sign and date it.*

f) *For details of the fee and ways to pay please contact the Patent Office.*

Mobile Security

A number of solutions exist for hosts to remain mobile while moving across different access networks (such as UMTS or WLAN). These solutions are based on the idea of allowing traffic flows to be redirected into the current location of the mobile node. In one solution, Mobile IPv6, the traffic flows are identified by a stable IPv6 address. In another solution, HIP, a public key (or a hash of a public key) identifies the traffic flows. In either case, a stable forwarding agent is required somewhere in the network for other nodes to contact the mobile node without previous knowledge of the current location of the mobile node.

In Mobile IPv6, this stable forwarding agent is called the home agent, and a security association must exist between the home agent and the mobile node for unauthorised location updates to be prevented. In HIP, there is no need for such a security association as the public key can be directly used to identify a particular node in a secure manner. However, in order for other nodes to learn the public key of the HIP-based mobile node, this public key must be stored in DNS in a secure manner. Therefore, in both cases the mobile node must be capable of securely performing transactions to its "home network", either for the purpose of talking to its home agent or updating the DNS to store its public key at the deployment phase.

Typically, the set-up of the security association for the home agent or the update of the DNS is performed in manual fashion. While parts of these operations have been automated, for instance through the use of a public key infrastructure, the authorisation step has to date remained a manual operation. In Mobile IPv6, this step involves the decision of whether the particular mobile node (even with a certificate from a trusted third party) is allowed to use a particular IPv6 address. This step is not easy to automate through public key infrastructure, given that the infrastructure would typically be unable to tell which IP address assignments are made in the network. In HIP, this is easier but requires the existence of a public key infrastructure and that it has made a determination of whether the mobile node is allowed to control the given domain name. The existence of such a public key infrastructure can be seen as redundant and unnecessary, given that the purpose of the DNS system is to act as a public key infrastructure – it would be strange to require another public key infrastructure to enter data into DNS.

The above technical problems lead to a service deployment problem in future networks. It is unacceptable from a business perspective to require manual work in order to set up each and every mobile node (out of millions) for the mobility service. Instead, it is preferred that the existing security mechanisms can be used to bootstrap whatever security may be required by the mobility mechanisms.

According to the present invention there is provided a method of securely initializing subscriber and security data in a mobile routing system when the subscribers are also subscribers of a cellular radio communication network, the method comprising:

within the mobile routing system, authenticating subscribers to the mobile routing system using an authentication procedure defined for the cellular radio communication network, collecting subscriber information from relevant nodes of the cellular radio network, and agreeing upon keys by which further communications between the subscribers and the mobile routing system can take place; and

using said subscriber information and keys in the provision of mobility services to subscriber mobile nodes and correspondent nodes.

According to a second aspect of the present invention there is provided a method of securely initializing subscriber and security data in a mobile routing system (such as Mobile IP) when the subscribers are also subscribers of a cellular radio communication network, the method comprising:

I. authenticating subscribers to the mobile routing system using the cellular radio communication network authentication,

II. collecting subscriber information related to the cellular radio communication subscriber from the relevant nodes of the cellular radio network,

III. agreeing upon a key or keys by which further communications between the subscriber and the mobile routing system can take place,

IV. communicating said subscriber information and keys to the mobile routing system,

V. using said subscriber information and keys in the offering of the mobility service to the mobile node and its correspondent nodes.

Step I may use underlying auth vs. rerun SIM authentication. For step III the keys may either be MIpv6 shared secrets between the MN and the HA, or HIP public keys which will be stored in DNS and used by the MN, forwarding agent and even peers.

For step I, the subscriber info can be a name or phone number which can be translated to a FQDN under the operator's domain. Then you can connect to, e.g. jsmith.sonera.fi. Then no administrator is needed at the operator site or the mobile node to set anything special up for this.

A subscriber database may be used, in the context of the so called subscriber certificates, to construct a FQDN which would be put in as an attribute of the produced certificate.

Cellular devices marketed by vendors typically contain a slot for a SIM card. The SIM cards are distributed by the operators, and they are used to authenticate the device to the network so that it can, for instance, make phone calls. Network operators have authentication servers which can verify the authenticity of the requests sent to it, and subscriber databases which contain phone number, name, and other information associated with a particular SIM card.

Our solution is to use the SIM card authentication, authentication servers, and subscriber databases to bootstrap the required security associations and DNS entries. The solution consists of the following steps:

Step 1. The client device establishes (IP) network connectivity by establishing a connection through GPRS, for instance. This step may involve the use of the SIM (or USIM) card for network access authentication; we consider the network access authentication to be an independent process, even if it uses the same SIM card as we use for another purpose. (But see later where we present a variation which can rely on network access authentication only.)

Step 2. The client device communicates with an authentication server in the operator's network to execute the SIM (or USIM) authentication with the server:

- The device sends its identity to the server.
- The server sends a challenge to the device.
- The device optionally verifies the authenticity of the server's challenge.

- The device sends a response to the server.
- The server verifies the authenticity of the device's response.
- The server optionally sends an acknowledgement back to the device.
- Both the device and the server establish shared session key(s), such as the USIM CK and IK.

Step 3. The client generates a public key pair.

Step 4. The client sends a message to the server, protected using the shared session key(s) established in Step 2. The message contains the following information:

- The public key of the device
- An optional signature of the device, made using the private key associated with the public key
- Optional desired parameters, such as a desired fully qualified domain name (FQDN).
- Optional shared secret (if provided, this part must be encrypted).

Step 5. The server verifies the authenticity of the client's message through the use of the shared session key(s) and optionally through the signature.

Step 6. The server collects information from the subscriber data base and the current contents of the local DNS zone and a Mobile IPv6 home agent or a HIP forwarding agent. This information may consist of, for instance,

- The name and postal address of the user associated with this SIM card.
- The telephone number associated with this SIM card.
- The existing FQDNs in the DNS (either for this particular subscriber or for others).
- The status of any mobility services established earlier for the particular subscriber or SIM card.

Step 7. The server makes a decision about a suitable FQDN and/or IP address which can be assigned to the device. For instance, the server can check the desired FQDN for consistency with the operator's domain name (e.g. sonera.net), the user's phone number or name (e.g., matti-virtanen.sonera.net), and the existence of possible previous entities with the same FQDN. The server also makes the necessary configurations in the following entities:

The local DNS zone: the selected FQDN and the associated public key is stored there. If HIP is used, the address of the operator's HIP forwarding agent is stored there as well.

- The operator's Mobile IPv6 home agent or HIP forwarding agent.
- The subscriber data base (possibly including a change in the billing information).

Step 8. The server communicates the configuration back to the device:

- The chosen FQDN and, optionally, IP address
- Optionally, the public key of some network node used by the device (such as a home agent)

Step 9. The node stores the received information. Note that this information has to be handled in a special way if a separation exists between a device and the user's credentials such as is common in phones and SIM cards inserted to them. Leaving the information in the device for use by any user (SIM card) would allow the use of this information by other users. This risk can be mitigated by storing the received information in the SIM, or storing it in the device in a manner which isn't accessible after another SIM has been inserted.

As a result, the device can now use mobility services in a secure manner: its public key and the forwarding agent can be retrieved from the DNS by anyone from the Internet and communications can flow to the device regardless of its current position and IP address. If a Mobile IPv6 home agent is used, the communications between the home agent and the device can be secured using the public key and/or shared secret.

Step 7 can be seen as the DNS name ownership test, and is in principle similar to the issues related to address ownership in IP mobility.

Current state of the art allows manual configuration as discussed earlier. This is unacceptable in the given business environment.

There exists proposals that make use of cell phone authentication in other contexts (e.g. RFC 3310), so the reuse of SIM authentication itself is not new. Here, however, we use it in a specific way for a specific application and combine information from the subscriber data base as well.

There exists proposals that make use of cell phone authentication even in the context of, e.g., Mobile Ipv6. However, these proposals use such authentication every time, and lack a mechanism to decide the IP addresses and FQDNs.

There also exists proposals to use cell phone and other legacy authentication mechanisms to generate so called subscriber certificates in general fashion, suitable for any application. However, our solution above avoids this step, and avoids the use of any PKI other than the resulting DNS system as a (weak form of) a PKI. Also, it is not clear that these general solutions can make the necessary authorisation decisions regarding FQDNs and IP addresses.

Standard protocols exist for making dynamic updates to DNS. However, currently these are secured with pre-provisioned shared secrets (DNS TSIG) or other mechanisms which can provide a shared secret, such as Kerberos (GSS TSIG) or secure DNS. All of these mechanisms today make the security decisions without regard to the specific entity that is making the request. This is insufficient, as it is necessary for a specific node to control its own IP address and DNS name, but not the addresses and names of other nodes. Our invention deals with this by combining the user data base and the authentication.

Embodiments of the invention would enable an easier deployment of mobility in heterogeneous networks.

A question which may need to be addressed is what happens if a device moves to a WLAN network. The same procedure can be applied if the cellular network is still available and if WLAN and cellular access are under the control of the same operator. If there are different, operators than the whole procedure should include negotiations between authentication servers of those operators.

Two different cases should be considered.
(a) Reuse of access-level authentication as such.
(b) Run another authentication between the mobility servers and the mobile node, but use the same credentials (e.g. SIM) as we did for the access.

The above concern may be relevant to case a. For case b, this is not an issue because whatever happens at lower layers is not relevant. For case a, a solution is to allow two different networks to use the same authentication, negotiate the authentication type,

transform information around. (This is happening as a part of IETF AAA and EAP protocols, and through 3GPP's work on 3G-WLAn interworking.)